Social- och hälsovårdsministeriets publikationer 2008:2

Utarbetande av en datasäkerhetsplan

Handbok för verksamhetsenheter inom social- och hälsovården

SOCIAL- OCH HÄLSOVÅRDSMINISTERIET

Helsingfors 2008

ISSN 1236-2050
ISBN 978-952-00-2507-6 (PDF)

Layout: AT-Julkaisutoimisto Oy

Sammandrag

Utarbetande av en datasäkerhetsplan. Handbok för verksamhetsenheter inom social- och hälsovården. Helsingfors 2008. 61 s. (Social- och hälsovårdsministeriets publikationer, ISSN 1236-2050, 2008:2)
ISBN 978-952-00-2507-6 (PDF)

Den centrala utgångspunkten i lagstiftning som gäller datasäkerhet är att säkerställa personlig integritet under alla omständigheter.

Datasäkerhet är en del av verksamhetsenhetens riskhantering. Datasäkerheten har en central betydelse i samtliga säkerhetssituationer; under normala förhållanden, i störningssituationer under normala förhållanden och i undantagsförhållanden. Datasäkerhet uppfattas ofta som skydd av information från obehörig användning. Den utgör dock en helhet som även täcker användbarhet och administration av uppgifterna. Tillhandahållare av offentliga och privata tjänster inom social- och hälsovården skall enligt lagen sörja för adekvat tillgång, användbarhet, skydd och integritet i fråga om handlingar och informationssystem och uppgifter som ingår i dessa samt för ändamålsenlig förstöring av uppgifter och material. En säker behandling av klientuppgifter accentueras ytterligare vid övergång till elektronisk behandling av klientuppgifter i tilltagande utsträckning.

Informationssamhällets sätt att verka och hot som hänför sig till detta är globala. Uttrycksform, källa och mål för datasäkerhetshoten är oberoende av etableringslandet. Hotet förverkligas dock lokalt så det krävs nationella åtgärder mot internationella hot. Nätverksbildning ökar den tillgängliga informationen och påskyndar beslutsfattandet. Problem uppstår ofta till följd av att alla användare inte har de kunskaper och färdigheter som nätverksbildningen förutsätter. Nätverken är allt oftare servicenätverk och hot mot datasäkerheten uppstår när uppgifter förflyttas mellan verksamhetsenheterna och på grund av verksamhetsenheters och aktörers rätt att använda varandras system.

Viktiga principer för datasäkerheten är användbarhet, integritet och konfidentiell natur. För administration och praktiska åtgärder har datasäkerhetsplaneringen och tillvägagångssätten indelats i följande helheter: administrativ säkerhet, personalsäkerhet, fysisk säkerhet, datakommunikationssäkerhet, driftssäkerhet, programsäkerhet, informationsmaterialsäkerhet och utrustningssäkerhet.

Administrativ datasäkerhet är en del av verksamhetsenhetens datasäkerhetspolitik där man har fastställt det administrativa systemet för datasäkerheten med dess rättigheter och ansvar. Verksamhetsenhetens högsta ledning beslutar

och ansvarar för datasäkerhetspolitiken. Med hjälp av datasäkerhetspolitiken fastställer ledningen verksamhetsenhetens principer och tillvägagångssätt för datasäkerheten och på grundval av detta fördelas ansvaret för den praktiska planeringen och arbetet inom varje område av datasäkerheten.

Denna handbok är avsedd för verksamhetsenheterna inom social- och hälsovården för att främja deras datasäkerhetsplanering. Målgruppen är särskilt sådana verksamhetsenheter inom social- och hälsovården som inte har egen personal för informationsadministration eller datasäkerhet. Handboken tar upp datasäkerhet delområdesvis så konkret som möjligt och beskriver viktiga begrepp inom datasäkerhet. Innehållsförteckningen har utarbetats så att den kan användas som hjälp vid upprättande av verksamhetsenhetens datasäkerhetsplan.

Handboken har på initiativ av beredskapsenheten vid social- och hälsovårdsministeriet utarbetats av en arbetsgrupp som tillsatts av säkerhetssektionen vid delegationen för hälso- och sjukvården under undantagsförhållanden i anslutning till ministeriet.

Nyckelord

handlingar, informationsadministration, informationssäkerhet, risker, riskhantering, undantagsförhållanden

Tiivistelmä

Tietoturvallisuussuunnitelman laatiminen. Opas sosiaali- ja terveydenhuollon toimintayksiköille. Helsinki 2008. 61 s. (Sosiaali- ja terveysministeriön julkaisuja, ISSN 1236-2050, 2008:2) ISBN 978-952-00-2507-6 (PDF)

Tietoturvallisuutta koskevan lainsäädännön keskeinen lähtökohta on yksityisyyden suoja ja sen turvaaminen kaikissa olosuhteissa.

Tietoturvallisuus on osa toimintayksikön riskienhallintaa. Tietoturvallisuudella on keskeinen merkitys kaikissa turvallisuustilanteissa; normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa. Tietoturvallisuus mielletään usein tietojen suojaamiseksi valtuudettomalta käytöltä. Se on kuitenkin kokonaisuus, joka kattaa myös tietojen käytettävyyden ja hallinnoinnin. Sosiaali- ja terveydenhuollon julkisten ja yksityisten palvelujen antajien ja järjestäjien tulee lain mukaan huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä sekä tietojen ja aineistojen asianmukaisesta hävittämisestä. Asiakastietojen turvallinen käsittely korostuu entisestään siirryttäessä yhä enenevässä määrin asiakastietojen sähköiseen käsittelyyn.

Tietoyhteiskunnan toimintatavat ja siihen liittyvät uhat ovat maailmanlaajuisia. Tietoturvauhkien ilmenemismuoto, lähde ja kohde ovat riippumattomia sijaintimaasta. Uhka toteutuu kuitenkin paikallisena, joten kansainvälisiä uhkia vastaan tarvitaan kansallisia toimenpiteitä. Verkostoituminen lisää saatavilla olevan tiedon määrää sekä nopeuttaa päätöksentekoa. Ongelmia syntyy usein siitä, että kaikilla käyttäjillä ei ole verkostoitumisen edellyttämiä tietoja ja taitoja. Verkostot ovat enenevästi palveluverkostoja, ja uhkia tietoturvallisuudelle syntyy tietojen siirrosta toimintayksiköiden välillä sekä toimintayksiköiden ja toimijoiden käyttöoikeuksista toistensa järjestelmiin.

Tietoturvallisuuden keskeiset periaatteet ovat käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuuden hallinnointia ja käytännön toimenpiteitä varten tietoturvallisuussuunnittelu ja menettelytavat on ryhmitelty yleisesti seuraaviin kokonaisuuksiin: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä laitteistoturvallisuus.

Hallinnollinen tietoturvallisuus on osa toimintayksikön tietoturvallisuuspolitiikkaa, jossa on määritelty tietoturvallisuuden hallintajärjestelmä oikeuksineen ja vastuineen. Tietoturvallisuuspolitiikasta päättää ja vastaa toimintayksikön ylin johto. Tietoturvallisuuspolitiikan avulla johto määrittelee toimintayksikön tietoturvallisuuden periaatteet ja toimintatavat, ja sen perusteella

jaetaan vastuut tietoturvallisuuden jokaisen osa-alueen käytännön suunnittelua ja työtä varten.

Tämä opas on tarkoitettu sosiaali- ja terveydenhuollon toimintayksiköille edistämään niiden tietoturvallisuussuunnittelua. Kohderyhmänä ovat erityisesti sellaiset sosiaali- ja terveydenhuollon toimintayksiköt, joilla ei ole omaa tietohallinto- tai tietoturvallisuushenkilöstöä. Oppaassa käsitellään tietoturvallisuutta osa-alueittain mahdollisimman käytännönläheisesti sekä kuvataan tietoturvallisuuden keskeisiä käsitteitä. Sisällysluettelo on laadittu siten, että sitä voidaan käyttää apuna laadittaessa toimintayksikön tietoturvallisuussuunnitelmaa.

Oppaan on laatinut sosiaali- ja terveysministeriön valmiusyksikön aloitteesta ministeriön yhteydessä toimivan poikkeusolojen terveydenhuollon neuvottelukunnan turvallisuusjaoston asettama työryhmä.

Asiasanat

asiakirjat, poikkeusolot, riskit, riskienhallinta, tietohallinto, tietoturva

Summary

Preparation of an Information Security Plan. A handbook for social and health care units. Helsinki, 2007. 61pp.(Publications of the Ministry of Social Affairs and Health, Finland, ISSN 1236-2050, 2008:2) 978-952-00-2507-6 (PDF)

An important starting point for the legislation on information security is privacy protection and the necessity of ensuring it under all circumstances.

Information security is part of the social and health care units' risk management. It is of major importance in all security situations: in normal conditions and incidences under them, and in emergency conditions. Information security is often understood as protection of information from unauthorised use. It is, however, an entirety that also covers the accessibility and management of information. Public and private social and health service providers shall according to the law see to the adequate availability, accessibility, protection and integrity of the documents and information systems and the data included in them, as well as that the data and material are destroyed appropriately. The importance of secure processing of client data is further emphasised with the increasing electronic processing of information concerning clients.

The ways how an information society functions and related threats are global. The manifestation, source and object of data security risks do not depend on the country of location. A threat however materialises locally, and therefore national measures are needed to respond to international threats. Networking increases the amount of information available and accelerates decision-making. Problems often arise out of the fact that all users do not have the knowledge and skills required for networking. Networks are increasingly service networks, and threats to information security arise in the context of transfer of information between units and in relation to the units' and actors' rights to use each other's systems.

The central principles of information security are accessibility, integrity and confidentiality. For the management of information security and practical measures the information security planning and procedures are generally grouped as follows: administrative and organisational security, personnel security, physical security, telecommunications security, operations security, software security, data security, and facilities security.

Administrative and organisational information security is a part of the unit's information security policy, which determines the system of management of information security with related rights and responsibilities. The top management of the unit decides and is in charge of the information security policy.

The management determines by means of the information security policy the principles and methods of information security, and the responsibilities for the practical planning and work in each sub-area are divided based on that.

The present handbook is intended for social and health care units to promote their information security planning. The target group is in particular those social and health care units that have not an information management or information security personnel of their own. The handbook deals with information security by sub-area as concretely as possible and describes the most important concepts of information security. The table of contents has been drawn up so that it can be made use of when drawing up the information security plan for the unit.

The handbook has been prepared by a working group set up by the security section under the Advisory Board for Health and Welfare in Emergency Conditions on the initiative of the Preparedness Unit of the Ministry of Social Affairs and Health.

Key words

documents, emergency conditions, information management, information security, risk management, risks

Innehåll

Förord

En datasäkerhetsplan utgör en del av verksamhetsenhetens riskhantering. Denna handbok är avsedd att främja datasäkerhetsplaneringen för verksamhetsenheterna inom social- och hälsovården. Målgruppen är i synnerhet sådana verksamhetsenheter inom social- och hälsovården som inte har en egen personal för dataadministration eller datasäkerhet. Handboken behandlar datasäkerheten på olika delområden så konkret som möjligt och beskriver viktiga begrepp inom datasäkerheten. Innehållsförteckningen är upplagd så att den kan användas som hjälp när verksamhetsenhetens datasäkerhetsplan utarbetas.

Datasäkerheten har en central betydelse i samtliga säkerhetssituationer; under normala förhållanden, i störningssituationer under normala förhållanden och under undantagsförhållanden. Datasäkerhet uppfattas ofta som skydd av information mot obehörig användning. Med datasäkerhet avses här dock en helhet som även täcker användbarhet och administration av uppgifterna. Kraven på datateknikens tillförlitlighet, funktionssäkerhet och användbarhet innebär att det är absolut nödvändigt att sörja för datasäkerheten.

Enligt offentlighetslagen ska myndigheterna sörja för adekvat tillgång, användbarhet, skydd och integritet i fråga om handlingar och informationssystem och uppgifter som ingår i dessa samt för ändamålsenlig förstöring av uppgifter och material.

Syftet med lagen om elektronisk behandling av social- och hälsovårdens klientuppgifter är att främja en säker behandling av klientuppgifterna. Lagen tillämpas på alla som tillhandahåller offentliga och privata tjänster. Handboken tar upp de lagenliga skyldigheterna vid planeringen av datasäkerheten.

Finansministeriets utvecklingsavdelning ger ut VAHTI-anvisningar för utvecklandet av datasäkerheten och styrningen av funktionerna. Till vissa delar kan anvisningarna användas även för att utveckla och upprätthålla de kommunala eller privata aktörernas datasäkerhet.

Handboken har utarbetats på initiativ av social- och hälsovårdsministeriets beredskapsenhet i anslutning till den arbetsgrupp som tillsatts av säkerhetssektionen vid delegationen för hälso- och sjukvården under undantagsförhållanden.

1 Datasäkerhet, dess lagenliga grund och begrepp

Den viktigaste utgångspunkten för lagstiftningen kring datasäkerhet är att skydda personlig integritet under alla omständigheter. Bestämmelser har därför utfärdats om datasekretess och arkivering, förhindrandet av obehörig användning samt kommunikationssäkerhet.

I ett samhälle som bygger på produktionsverksamhet och dess konkurrenskraft måste i lagen föreskrivna samt i övrigt konfidentiella och sekretessbelagda uppgifter om personer, organisationer och verksamhetsenheter skyddas mot obehörig användning. En väsentlig och oskiljaktig del av riskhanteringen är att klassificera uppgifterna och definiera deras värde med tanke på individen eller samfundet.

Integritetsskyddet tryggas i grundlagen. Grunden för dataskyddet är personuppgiftslagen. I lagarna om social- och hälsovården fastställs dataskydds- och sekretessförfarandet. Programmen och informationsinnehållet skyddas i lagen om upphovsrätt. Strafflagen innehåller bestämmelser om brott mot datasäkerheten.

I § 24 i lagen om offentlighet i myndigheters verksamhet (621/1999) fastställs de sekretessbelagda myndighetshandlingarna. När dessa handlingar skapas, ändras, förflyttas, arkiveras, förstörs och på annat sätt behandlas är det väsentligt att behandlingen av all information och alla dokument i de sekretessbelagda handlingarna är enhetlig enligt säkerhetsklassificeringen. En handling ska säkerhetsklassificeras när den är sekretessbelagd enligt 24 § 1, 2, 5, 7, 8, 9, 10 eller 11 punkten i lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen). Dessa handlingar behandlar uppgifter som är ömtåliga och sekretessbelagda med tanke på samhällets säkerhet eller vissa centrala uppgifter av allmänt intresse.

Handlingar som inte berörs av offentlighetslagen är bl.a. tjänstemännens anteckningar och handlingar som skaffats för intern utbildning samt tjänstemännens privata brev.

Den främsta lagstiftningen kring datasäkerhet presenteras i bilaga 1.

Finansministeriets avdelning för administrationsutveckling utfärdade 19.1.2000 en anvisning om säkerhetsklassificeringen och anteckningen av sekretessbelagda uppgifter och handlingar (FM 5/01/2000).

Viktiga principer för datasäkerheten är användbarhet, integritet och konfidentiell natur.

Användbarhet innebär att informationen alltid är tillgänglig när den behövs inom en förhandsbestämd tid. Den utrustning och de program som informationen behandlas med påverkar användbarheten.

Integritet betyder att informationen förblir oförändrad när uppgifterna behandlas, förmedlas från en plats till en annan eller arkiveras.

Konfidentiell natur betyder att obehöriga inte får en möjlighet att se, ändra, förstöra eller på annat sätt behandla dokumentet eller informationen.

Elektronisk kommunikation blir allt vanligare och begreppen kring datasäkerhet omfattar därför även definitionen ***obestridlighet***. Obestridlighet betyder en egenskap och metod hos en uppgift med vilken systemanvändaren identifieras, och med vilken man försäkrar sig om att uppgiften är riktig och att händelsen är juridiskt bindande.

Med datasäkerhet avses att information skyddas mot obehörig användning, ändring och förstöring. Datasäkerhet innebär även att informationens användbarhet kontrolleras. Det innebär skydd, kontroll och riskhantering av information och elektroniska tjänster, enskilda datasystem samt datakommunikation genom administrativa och tekniska åtgärder.

Datasäkerhet indelas enligt följande:

- administrativ säkerhet
- personalsäkerhet
- fysisk säkerhet
- datakommunikationssäkerhet
- driftsäkerhet
- programvarusäkerhet
- informationsmaterialsäkerhet
- utrustningssäkerhet

Administrativ säkerhet: organisering av verksamheten, personalens uppgifter samt anvisningar, ansvar, utbildning och övervakning.

Personalsäkerhet: personalens tillförlitlighet och lämplighet, rättshantering, vikariearrangemang samt anställningsarrangemang.

Fysisk säkerhet: datateknikens användningsmiljö, fastighetens byggtekniska säkerhet, kontrollteknik, kontroll och bevakning samt personalskydd.

Datakommunikationssäkerhet: dataöverföringsförbindelsernas användbarhet, skydd och kryptering av dataöverföringen, användarnas identifiering och nätkontroll.

Driftsäkerhet: användning i trygga förhållanden, teknisk funktionskontroll, åtkomsträttigheter, kontroll av användning och logg, säkerhetsåtgärder för programstöd, underhåll och service, säkerhets- och skyddskopiering samt störningsrapportering.

Programvarusäkerhet: skyddsegenskaper hos operativsystem, utrustnings- och nyttoprogram samt övriga program och tillämpningar, kontroll- och loggförfaranden samt säkerhetsåtgärder kring programunderhåll och uppdateringar.

Datamaterialsäkerhet: uppgifternas och datamaterialets användbarhet, riktighet samt sekretess i alla skeden av dess livslängd.

Utrustningssäkerhet: utrustningens användbarhet, funktion, underhåll samt utrustningens och tillbehörens tillgänglighet och tagning ur bruk.

2 Hot mot datasäkerheten

Problem med datasäkerheten uppstår på grund av

- användningen av internet utan uppdaterat antivirusprogram
- användningen av trådlösa nät utan kryptering
- problem med tillgången på programstöd
- osäker datamiljö
- bristfällig hantering och övervakning av åtkomsträttigheter och behörighetstilldelning
- problem med datahanteringsutrustning och operativsystem
- avsiktliga eller oavsiktliga fel eller förseelser
- bristfällig inskolning och utbildning
- bristfälliga bekämpningssystem mot fientliga program och virus

Informationssamhällets arbetsmetoder och hot är globala. Formen, källan och målet för hoten mot datasäkerheten är oberoende av etableringsland. Hotet framträder emellertid lokalt, och därför behövs det nationella åtgärder mot internationella hot. Nätverksbildningen ökar mängden tillgänglig information och leder till snabbare beslut. Problemen uppstår ofta därför att alla användare inte har de kunskaper och färdigheter som förutsätts vid nätverksbildning. Alltid kan man inte heller bedöma värdet av eller riktigheten i de uppgifter som finns på nätet. Nätverken utgörs allt mer av servicenätverk, och hoten mot datasäkerheten uppstår vid överföringen av information mellan verksamhetsenheterna samt i anknytning till enheternas åtkomsträttigheter till varandras system. Hanteringen av rättigheterna sker i snabb takt enligt situation. Nivån på de olika parternas datasäkerhet kan avvika rätt mycket, och det är inte alltid problemfritt att reda ut skillnaderna. Det är viktigt att koncentrera sig extra mycket på ansvarsfördelningen för att datasäkerheten ska kunna tryggas i samarbete av den här typen. Å andra sidan skapar nätverksbildningen förutsättningar för en bättre datasäkerhet därför att informationen om bra och effektiva arbetsmetoder sprids snabbt.

De mest sannolika hoten mot datasäkerheten och därmed riskerna härrör från användarna. Problemen med datasäkerheten kan uppstå oavsiktligt eller avsiktligt. Användarna kan agera rätt självständigt och åsidosätta de administrativa och tekniska lösningar för datasäkerheten som enheten erbjuder. Man får inte ge avkall på datasäkerheten på bekostnad av lönsamheten.

Okontrollerad användning av e-post eller internet kan leda till problem för en enskild arbetsstation eller enhetens server om användaren av misstag öppnar

en fil som innehåller ett fientligt program. Beroende på datasystemet kan man bekämpa virus och fientliga program på enskilda arbetsstationer med antivirusprogram, med virusbekämpningsprogram på servern eller med brandmurar och program som täcker hela systemet.

Ett betydande hot som den stora rörligheten lett till är otillåten åtkomst till information och program i utrustningen. Datahanterings- och kommunikationsutrustning används i stor utsträckning utanför verksamhetsenheten. De vanligaste är bärbara datorer (laptop), telefoner, kommunikatorer och fickdatorer (PDA-datorer) samt usb-minnen. Datahanteringsutrustning, bl.a. servrar, kan vara belägna i en utomstående serviceproducents egna lokaler. Om utrustningen försvinner kan informationen hamna i händerna på obehöriga personer.

När tekniken utvecklas kan användarens verksamhet utgöra en datasäkerhetsrisk. Det beror på att användningen av program och utrustning är svårbegriplig. Problemet kan minskas med ordentlig inskolning och utbildning.

Andra hotbilder är brister i programstödet och fel i utrustningen. Vid riskkontrollen ska även problemen i den fysiska miljön beaktas, som t.ex. elavbrott, eldsvåda och vattenskador.

Hot mot datasäkerheten uppstår när användaren inte behärskar sin utrustning, användningsmetoder, operativsystem, program eller programvara, för då ökar riskerna till följd av eventuella felfunktioner.

Hot mot datasäkerheten uppstår även när användaren arbetar i en miljö där obehöriga personer obehindrat kommer åt t.ex. att se information på dataskärmen. Skrivaren eller faxapparaten ska placeras så att utomstående inte kommer åt konfidentiellt material i apparaterna.

Även om en allt större del av det material som lyder under dataskyddet hanteras i elektronisk form kommer en del av uppgifterna alltjämt att hanteras i pappersform eller muntligt. Därför är det viktigt att alla är medvetna om sitt eget ansvar vid hanteringen av konfidentiell information i varje användarmiljö och om de tillvägagångssätt som lagen kräver.

3 *Anvisningar för att utarbeta en datasäkerhetsplan*

En datasäkerhetsplan omfattar anordnandet av verksamhetsenhetens förvaltning av datasäkerhet, datahanteringsmetoder och användningskontroll, datasäkerhetsaspekter vid anskaffningen av utrustning och system, verksamhetens kontinuitet samt upprätthållandet av datasäkerhetsplanen.

I planen fastställer enheten den aktuella informationens konfidentiella natur, hanteringssätt och åtkomsträttigheter, arkivering, förstöring samt förfaringssätt i störningssituationer under normala förhållanden samt under undantagsförhållanden angivna i beredskapslagen.

Vid planeringen utarbetas en beskrivning av datahanteringsprocesserna, av riskbedömningen och åtgärderna för att eliminera, minska eller tåla riskerna. Denna beskrivning utnyttjas när planen utarbetas och åtgärds- och investeringsprogrammet i planen förbereds.

Datasäkerhetsplanen ska även omfatta en beskrivning av personalens utbildning.

I datasäkerhetsplanens kontinuitetsplan (beredskapsplan) beskrivs verksamhetsenhetens åtgärder i sådana situationer där datahanteringen förhindrats av normala orsaker, t.ex. när eltillförseln avbrutits eller ett fel i utrustningen upptäckts, och informationen inte kan hanteras på normalt sätt. För dessa eventualiteter ska enheten bedöma prioriteringsklassificeringen vid datahanteringen samt vilka metoder som ska användas för att spara och återställa informationen när problemsituationen korrigerats.

I datasäkerhetsplanen ska arbetsmetoderna fastställas och ansvariga personer i situationer med datasäkerhetsförseelser utses.

Enheten ska utse personer som är ansvariga för upprätthållandet av datasäkerhetsplanen och övervakningen av datasäkerheten.

Stommen i datasäkerhetsplanen presenteras nedan:

INNEHÅLLET I DATASÄKERHETSPLANEN

4 Administrativ datasäkerhet

Den administrativa datasäkerheten utgör en del av enhetens datasäkerhetspolicy, där datasäkerhetens hanteringssystem inkl. rättigheter och ansvar fastställs.

Enhetens högsta ledning ansvarar för och beslutar om enhetens datasäkerhetspolicy. Med hjälp av enhetens datasäkerhetspolicy fastställer ledningen principerna och tillvägagångssätten för enhetens datasäkerhet. I datasäkerhetspolicyn fastställs:

- avsikten och målen för datasäkerheten
- enhetens principer för datasäkerheten
- datasäkerhetsprinciperna för enhetens tekniska system
- hanteringssystemet för datasäkerheten
- ansvar för datasäkerheten
- hur datasäkerheten verkställs
- anvisningar
- utbildning
- organisera uppföljningen
- datasäkerhetsprinciper för utlagda tjänster
- konsekvenserna av förseelser mot datasäkerheten
- information.

4.1 Organisera hanteringen av datasäkerheten

Datasäkerheten utgör en fast och väsentlig del av enhetens värdemiljö, ledarskap och riskhantering. Därför ska administreringen av datasäkerheten inte läggas ut.

Alla anställda bär ansvar för datasäkerheten i anknytning till sina egna arbetsuppgifter. Arbetsgivarens skyldighet är att se till att de anställda får den handledning och utbildning som de behöver för sina uppgifter och för sina gränssnitt, användarsystem och operativsystem.

Ansvaret för datasäkerheten ska ges till personer med tillräckliga kunskaper och praktiska möjligheter att ta hand om den. Enheten ska utse antingen en ordinarie datasäkerhetschef eller en som sköter uppdraget vid sidan av sitt ordinarie arbete, samt personer som ansvarar för datasäkerheten på respektive

ansvarsområden beroende på enhetens storlek och förvaltningsmodell. Det är viktigt att se till att uppdrag i anknytning till tekniskt dataskydd och förvaltningen av datasäkerheten inte ges till samma personer.

För att minimera riskerna och hoten mot datasäkerheten ska personalen förbinda sig att följa enhetens datasäkerhetskultur och praktiska åtgärder. Det förutsätter att personalen sätter sig in i enhetens datasäkerhetsanvisningar. En modell över datasäkerhetsanvisningarna samt en blankett för anmälan om förbindelse presenteras i bilaga 2 och 3.

Utöver ansvaret för den allmänna utvecklingen och uppföljningen av datasäkerheten ska ansvaret fördelas även när det gäller operativsystem, program och programvara samt hårdvara och utrustning. Med ansvarsfördelning avses här att enheten för varje systemhelhet eller utrustningshelhet utser en s.k. ägare. Ägarens uppgift är att ansvara för de aktuella systemens, programmens eller utrustningshelheternas funktion och upprätthålla datasäkerhetsegenskaperna tillsammans med enhetens övriga experter.

4.2 Planer hänförliga till datasäkerhet

Den viktigaste planen hänförlig till datasäkerheten är enhetens datasäkerhetsplan. Enligt behov utarbetas för enheten en återhämtningsplan eller beredskapsplan. Återhämtningsplanen utgörs av anvisningar i situationer där datasystemet antingen planmässigt eller på grund av något överraskande och oförutsägbart problem är ur bruk. I planen fastställs databehandlingsförfarandet och ansvariga personer under avbrottet. Därtill ges instruktioner om hur datasystemet tas i bruk efter en problemsituation eller ett avbrott.

Övriga planer hänförliga till datasäkerheten kan vara bl.a. en extern utvärderingsplan i anslutning till datasäkerhetshantering, -användning och datasystem samt en utbildningsplan.

4.3 Samarbete med utomstående

Enheten ska ha godkända anvisningar för tillvägagångssättet när det gäller externa serviceproducenter. När enheten lägger ut funktioner ska man se till att serviceproducenten känner till enhetens datasäkerhetspolicy och –praxis när det gäller serviceobjektet. Den enhet som köper upp tjänsten ska också kontrollera att det serviceproducerande företaget har egna uppdaterade datasäkerhetsanvisningar.

Utomstående personer eller personer i företag som ingått avtal med enheten ska förbinda sig vid enhetens datasäkerhetspraxis på samma sätt som enhetens

egen personal. På detta sätt kan man garantera att sekretessbelagd information inte hamnar i obehöriga personers händer.

Till spelreglerna för samarbetet hör även att förhindra s.k. ”social hackerverksamhet”. Detta innebär att enhetens anställda både på arbetsplatsen och utanför den ska agera så att ingen del av en för enheten värdefull och konfidentiell information hamnar i händerna på obehöriga, utomstående personer.

Anvisningar om praktiska tillvägagångssätt och dataskydd samt kryptering när det gäller datasäkerheten utgör grunden för utvecklandet och upprätthållandet av datasäkerhetskulturen. Enhetens högsta ledning bär ansvar för anvisningarna och informationen om dem.

5 Personalsäkerhet

Åtgärder kring personalsäkerheten gäller riskhanteringen hänförlig till personalen. De främsta punkterna för diskussion är avhängighet av nyckelpersoner, personalens tillförlitlighet, anställningsmetoder, personalutbildning och tillvägagångssätt när det gäller utomstående arbetare.

Målet med personalsäkerheten är att minska risken för att personalen begår misstag när det gäller material som ska skyddas samt risken för stöld, bedrägeri och missbruk.

Genom personalsäkerhet kan man bidra till att bevara och upprätthålla enhetens främsta värderingar. Redan i rekryteringsskedet ska man beakta de anställdas lämplighet för sitt uppdrag. Samtidigt som man beslutar om de anställdas arbetsbeskrivning och arbetsuppgifter ska man beakta ersättararrangemangen, rätten till information, åtkomsträttigheter, skyddsförfaranden samt säkerhetsutbildning och övervakning.

Typiska hot mot personalsäkerheten är:

- bristfälliga arbetsmetoder
  - datasäkerhetsanvisningar, information om regler och bestämmelser, brister i övervakning och utbildning
- oavsiktliga handlingar
  - användningsfel
  - operativa fel
  - oavsiktlig virusspridning
  - överbelastning av personalen
  - underhållsfel
  - problem vid serviceåtgärder
- avsiktliga handlingar
  - förstöring av datamaterial
  - intrång i databaser
  - tillgrepp av information
  - ändring av datamaterial
  - olovlig avlyssning och iakttagelse av datanät
  - agera med andras åtkomsträttigheter
- oöverstigligt hinder
  - förlust av nyckelperson.

5.1 Avhängighet av nyckelpersoner

Avhängighet av nyckelpersoner innebär att det på olika nivåer i enheten finns anställda vilkas know-how är av avgörande betydelse för upprätthållandet av enhetens verksamhet och för att resultat ska kunna nås. Om en eller flera nyckelpersoner plötsligt eller samtidigt är frånvarande eller försvinner från arbetsplatsen antingen för en längre tid eller bestående kan det medföra stora kostnader för enheten om motsvarande tjänst eller kunnande måste skaffas externt. Det är viktigt att det finns en ersättare med tillräckliga befogenheter utsedd för varje nyckelperson.

Omfattningen och den unika karaktären av nyckelpersonernas arbetsfält ska bedömas enligt riskhanteringsmetoder. Man ska i synnerhet beakta effekterna av nyckelpersonens frånvaro på eventuella avbrott i enhetens livsviktiga och för kontinuiteten centrala samt ekonomiskt betydande funktioner.

5.2 Anställningar

En bedömning av tillförlitligheten hos personer som anställs vid enheten är viktig i synnerhet när man rekryterar en person för uppdrag som är centrala och kritiska med tanke på enhetens riskhantering. Utöver den sökandes tjänsteintyg kan det vara ändamålsenligt att begära information av personens tidigare arbetsgivare eller be polisen om en säkerhetsrapport. Enligt gällande lagstiftning krävs det alltid den sökandes samtycke till detta. Enligt lagen ska bakgrunden till personer som arbetar med barn alltid utredas, och i detta fall krävs inget samtycke av den sökande.

Arbetsgivaren kan också förutsätta att den sökande ger sitt samtycke till lämplighetstest eller drogtest. Emellertid kan arbetsgivaren inte tvinga den sökande till någotdera testet. Det vilar på arbetsgivarens ansvar att utreda att testmetoderna håller tillräckligt hög kvalitet.

5.3 Personalens tillförlitlighet och förbindelser

Syftet med personalsäkerheten är att få de anställda att agera på överenskommet sätt. Utgångspunkten är ett ömsesidigt förtroende mellan de anställda och arbetsgivaren. För att enhetens främsta värderingar ska kunna iakttas förutsätts det att enhetsledningens verksamhetspolicy och strategier för enheten finns som stöd för uppgifterna och arbetet, och att dessa kompletteras av mer detaljerade anvisningar om tillvägagångssätt. För att främja och upprätthålla en datasäkerhetskultur är det ändamålsenligt att alla anställda förbinder sig vid de

främsta tillvägagångssätten. I förbindelsen kommer man överens om spelreglerna för datasäkert arbete. Spelreglerna anger tydligt vad som är tillåtet och vad som inte är tillåtet.

Den anställdas tillförlitlighet kan utvärderas regelbundet under anställningen. I första hand görs utvärderingen av den anställdas chef, men även utomstående test kan utnyttjas. En utvärdering genom test kräver alltid den anställdas samtycke.

5.4 Personalutbildning

Det räcker inte med regler, instruktionsbrev och arbetsanvisningar för att skapa och upprätthålla en datasäkerhetskultur. Personalen måste också erbjudas inskolning och utbildning. Det är önskvärt att enhetens egen personal ger utbildningen. Om enheten använder sig av köpta tjänster ska enheten se till att innehållet i utbildningen motsvarar arbetsgivarens syn på enhetens verksamhetspolicy, strategier och arbetsmetoder.

5.5 Externa arbetstagare och inköpstjänster

Med externa arbetstagare avses personer som arbetar för enhetens räkning i något annat företag eller samfund, dvs. producerar olika tjänster för enheten. De kan också vara självständiga företagare som arbetar antingen i enhetens lokaler eller i andra lokaler än hos den enhet som beställt tjänsten. När det gäller externa arbetstagares datasäkerhet är tillvägagångssättet precis detsamma som för den egna personalen när det gäller lagstadgade och avtalsrättsliga detaljer. Man bör fästa extra mycket uppmärksamhet vid avtalspolitiken och tillvägagångssätten när den externa arbetstagaren arbetar i något annat land än Finland och det aktuella landets lagstiftning avviker från finländsk lagstiftning.

5.6 Förfarandet vid avslutad anställning

När den anställdas anställning upphör är det arbetsgivarens och chefens skyldighet att tillsammans med den anställda se till att all information som tillhör arbetsgivaren på den anställdas arbetsstationer i personligt bruk eller på de elektroniska datalagringsutrustningarnas hårdskivor och minneskort sparas och att konfidentiellt datamaterial inte hamnar i händerna på obehöriga personer. När informationen öppnas och tas tillvara ska man beakta bestämmelserna om tillvägagångssätten i lagen om integritetsskyddet i arbetslivet. Datasystemens

åtkomsträttigheter och passerkontrollrättigheterna ska återtas samma dag som anställningen upphör. I informationssäkerheten när en anställd avgår ingår även att arkiven och skribordslådorna i den anställdas arbetsrum städas och all information som inte hör till arbetsgivaren förstörs enligt anvisningarna för respektive skyddsnivå. Separata anvisningar ska utfärdas för hur informationen på arbetsstationernas hårdskivor och annan datalagringsutrustning ska förstöras.

6 Fysisk datasäkerhet

Fysisk datasäkerhet omfattar säkerhet och skydd av arbetslokaler. Syftet är att genom riskhantering förhindra skada på enhetens lokaler genom att minimera hoten mot dem.

Fysisk säkerhet innebär skydd av enhetens produktions- och kontorslokaler så att man förhindrar att enhetens information förstörs, skadas eller hamnar i händerna på obehöriga personer. Detta datasäkerhetsområde omfattar passerkontroll, teknisk kontroll och bevakning, bekämpning av inbrottsskador, brand-, vatten-, el-, värme- och luftkonditioneringsskador samt säkerhet för försändelser som innehåller informationsmaterial.

Kartläggningen och identifieringen av hot gäller:

- fastighetens säkerhet:
- säkerhetsarrangemang kring arbets- och anläggningslokaler
- kundservicelokalernas säkerhet
- reservkraftsystem.

6.1 Strukturellt skydd och kontroll

Genom strukturellt skydd, kontroll och bevakning strävar enheten efter att skydda all information som enheten äger och administrerar mot eventuella inkräktare. Med skyddskonstruktioner, som t.ex. äkta och slagtåliga fönsterglas, försöker enheten fördröja inkräktarens intrång. Med bevakning försöker man förkorta svarstiden för larmet till väktare och andra som står för lokalens säkerhet.

Fastighetsbevakningens uppgift är att försöka förhindra eller avslöja skadegörelse på fastigheten samt fel i fastighetens el-, vatten-, värme- och luftkonditioneringssystem. Enhetens verksamhet får inte under några som helst omständigheter utsättas för fara på grund av att lokalerna inte kan användas eller att information eller informationssystem som är livsviktiga för enhetens verksamhet förstörs eller blir obrukbara.

6.2 Låsning och passerkontroll

Låsningen och passerkontrollen ska begränsa utomstående personers tillträde till lokaler där sådan information förvaras eller hanteras som inte får hamna i händerna på obehöriga personer. Utöver utomstående personer kan man vid behov begränsa passerrättigheterna även för enhetens egen personal.

6.3 Brandskydd

Brandskyddet ska förhindra eldsvådor samt vid en eventuell eldsvåda minimera skadorna på lokaler, apparater, datasystem och information.

Det är viktigt att notera att en temperatur på bara 60 °C kan förstöra data på elektroniska lagringssystem (disketter, CD-ROM-skivor m.m.) antingen delvis eller helt. Säkerhetskopior och –lagringar ska därför förvaras i brandsäkra skåp.

Vid val av brandsläckare är det också viktigt att beakta att det finns brandsläckare avsedda speciellt för släckning av elbränder. Brandsläckningssystemen ska väljas med tanke på att datasystemutrustningen i lokalerna ska kunna användas även efter branden och släckningsåtgärderna.

7 Datakommunikationssäkerhet

Med datakommunikationssäkerhet avses störningsfri kommunikation.

Datakommunikationssäkerheten omfattar bl.a. monteringen av datakommunikationsutrustning, förteckning av utrustningen, underhållsarrangemang samt kontroll och dokumentering av ändringar.

Ostörd datakommunikation kräver webbkontroll, kommunikationssäkring, observation av betydelsefulla händelser (t.ex. exceptionellt stor e-postkommunikation), test av datakommunikationsprogram samt registrering av problemsituationer.

För att kunna identifiera hoten ska man se till:

- webbkontrollen (hantering, routing, åtkomst, reservarrangemang)
- att krypteringen fungerar
- att brandmursprogrammet är uppdaterat
- att externa förbindelser och tjänster fungerar.

7.1 Nätets säkerhet

När enhetens datakommunikationsnät planeras och byggs upp ska man bedöma hur kritiska de nödvändiga förbindelserna mellan arbetsstationerna och servrarna är med tanke på sårbarheten hos enhetens funktioner i eventuella fel- eller störningssituationer. Effekterna av funktionsstörningar kan minskas genom att man bygger upp ramnät eller dubblerar förbindelserna.

I datakommunikationen via trådlösa nät ska man notera behovet av kryptering när nätet används för förmedling av konfidentiella uppgifter. Detta gäller även den utgående kommunikationen eller den ingående kommunikationen via olika nät.

7.2 Tryggandet av energitillförsel

En väsentlig detalj i upprätthållandet av datakommunikationssäkerheten är att trygga energitillförseln. Vid riskkarteringen ska man kartlägga de datasystem som är kritiska för verksamheten (servrar, routrar och kopplingar) enligt följande:

- inga driftavbrott tillåts
- korta driftavbrott på några sekunder tillåts
- driftavbrott på några minuter tillåts
- driftavbrott på några timmar tillåts.

De kritiska servrarna får gärna besitta en sådan teknik att servern startar av sig själv efter ett elavbrott.

När datanätet byggs upp ska man beakta nätets känslighet för störningar i eltillförseln och överspänningstoppar. Det är möjligt att undvika största delen av störningsfaktorerna genom att välja kablar av hög kvalitet och skilja datakommunikationskablarna från andra elkablar.

Vid riskklassificeringen för datasystemnätet kan följande gruppering följas:

- adb-maskinrum
- routrar och kopplingar på routinglinjerna
- viktiga enskilda användarpunkter
- övriga betydande funktionshelheter
- vanliga användare.

Utgångspunkten vid planeringen av energitillförseln kan vara att alla routrar, kopplingar och arbetsstationer inte nödvändigtvis behöver ingå i en obruten strömkrets. Det innebär att all datautrustning inte förses med UPS-enheter, dvs. backupbatterier helt enkelt därför att investeringarna och underhållskostnaderna för att säkerställa eltillförseln är stora i relation till nyttan.

Största delen av datautrustningen ska dock kopplas till reservkraftaggregatet. Det kan vara bra att planera eltillförseln från de allmänna näten så att enheten kan få energi från två olika transformatorkretsar.

Utgångspunkterna för planeringen av adb-maskinrummet kan beakta följande:

- dubblerade system
- UPS-utrustning (målet för reservdrift minst 30 minuter).
- säker tillgång på startström från reservkraftgeneratorerna
- kylsystemets elmatning och att säkerställa den
- säkerhetsbelysning och att säkerställa den
- brandlarmsystemen och att säkerställa eltillförseln till dem
- släckningssystemen och dessas anpassning till objektet
- brottsanmälningssystem och att säkerställa eltillförseln till det
- klassificeringssystem och eltillförseln till det (om ellås används)
- passerkontrollsystem och att säkerställa eltillförseln till det
- tv- och videoövervakningssystem och att säkerställa eltillförseln till det
- rökfångarsystem och att säkerställa eltillförseln till det

7.3 E-post

E-posten förmedlas främst via internet. Därför är e-post inte ett säkert sätt att sända konfidentiellt material, ifall meddelandet inte krypteras hela vägen från avsändare till mottagare. Om man använder sig av olika typer av kryptering, ska krypteringskoden vara minst 132 bit för att den ska vara svårare att knäcka.

För att trygga e-postsystemet ska brandmuren använda sig av bl.a. följande metoder för att bekämpa virus och spam:

- ***Förhindra att vidareförmedla ett meddelande (reläande).*** E-postsystemet förmedlar inte automatiskt externt meddelanden som härrör från andra än enhetens egna adresser och vars mottagaradress inte är en e-postadress inom enheten.
- ***Inkommande meddelanden från okända funktionsområden eller datorer.*** E-postservern genomför en namnkontroll. Om systemet inte identifierar det avsändande funktionsområdet eller datorn förhindras förmedlingen automatiskt tills systemet har fastställt avsändaren.
- ***E-postförmedlingsspärr*** E-postsystemet förmedlar inte e-post från servrar eller enskilda arbetsstationer som sänder spam eller vars huvudman är känd för att stödja spamavsändare.
- ***E-postförmedlingsspärr på datorer som ständigt byter webbadress (dynamiskt tilldelad).*** E-postsystemet förhindrar förmedling av e-post från datorer som ständigt byter webbadress.
- ***Åtkomstförteckning enligt server.*** Vid behov kan man programmera e-postsystemet med åtkomstförteckningar enligt server för att bekämpa spam. För att behärska nätbelastningen kan man med hjälp av förteckningen tillfälligt eller permanent stänga av separata funktionsområden, avsändare, mottagare, enskilda webbadresser eller hela undernät.
- ***Filtrering för att trygga kapaciteten.*** Genom att observera e-postserverns loggar i realtid kan man upptäcka e-postförsändelser som avviker från det normala. En alltför stor belastning av kapaciteten känns ofta igen på ovanligt långa sessionstider till e-postservern, exceptionellt antal meddelanden från samma källa eller ett stort antal mottagare av ett meddelande.
- ***Begränsa meddelandenas storlek och antal bifogade filer.*** E-postmeddelandenas storlek och antal bifogade filer kan begränsas om serverkapaciteten förutsätter det och begränsningarna har angivits.
- ***Identifiering och radering av fientliga program.*** Följ med filtyper som brukar användas för förmedling av fientliga program. De fientliga programmen kan raderas från meddelandena eller meddelandet som innehåller ett fientligt program kan förstöras.

- ***Identifiering och filtrering av spam.*** Ett meddelande som klassificeras som skadligt i en innehållsmässig analys ska alltid märkas som spam. Meddelandet ska filtreras och sändas till mottagarens e-post. E-posten kan också filtreras till ett separat karantänområde där det kan läsas av mottagaren, eller mottagaren kan informeras om meddelandet på annat sätt inom skälig tid.
- ***Fördröjning av e-post.*** För att identifiera fientliga program i e-postmeddelanden kan man vid behov fördröja e-posten till mottagaren så länge som det behövs för identifieringen.

Informationen om enhetens filtreringsmetoder ska finnas beskriven och tillgänglig för alla.

8 Driftsäkerhet

Driftsäkerheten omfattar säkerhet kring användningen av datatekniken, miljön, datahanteringen och kontinuiteten samt kring stöd-, underhålls,- utvecklings- och servicefunktionerna. (Målet är hantering och underhåll av datorer, programvara och daglig användning av datakommunikations-enheterna.

8.1 Hantering av miljön

Hanteringen av miljön (IT-infrastrukturen) beskrivs i handboken för enheterna. I handboken beskrivs datapersonalens dagliga rutinmässiga uppgifter och metoder för att lösa problem i anknytning till maskinvaru-, programvaru- och datakommunikationsmiljön. Dessa är till exempel:

- definition av rättigheter
- förfarandet vid byte av standardlösenord
- förfarandet vid en ändring av datasystem
- godkännande- och förflyttningsförfarandet när system, apparater osv. tas i bruk
- systemprogram- och reparationsuppdateringar
- planering och information vid serviceavbrott
- säkerhetskopiering
- skyddskopiering
- synkronisering av systemklockor
- anordnande av användarstöd
- störningsrapportering
- skyddsmetoder för systemdokumentation
- skydd av systemets hanterings- och analysverktyg
- övervakning av apparat-, kopplings- och driftslokaler.

8.2 Hantering av åtkomsträttigheter och fullmakter

Hanteringen av åtkomsträttigheter och fullmakter gäller fastställandet av principerna för åtkomsträttigheterna. Här beaktas nödvändiga begränsningar för varje datasystemanvändare.

Åtkomsträttigheter och –fullmakter för varje datasystem beviljas separat till användare och systemadministratörer. Ett register ska föras över rättigheterna och fullmakterna. Anvisningar ska utarbetas över ändringar och upphävandet av rättigheter och fullmakter.

Separata instruktioner ska utarbetas om lösenordspraxis. Anvisningarna ska understryka lösenordets kvalitet, dvs. att lösenordet ska bestå av minst åtta tecken och att det ska innehålla både gemena och versaler, siffror och specialtecken. Klara anvisningar ska ges om hur lösenorden ska sparas.

8.3 Arbete under resor, distansarbete och distansanvändning

Enheten ska bestämma vilka arbetsuppgifter som kan utföras på distans. Arbetsgivaren fastställer vilka fysiska säkerhetsfaktorer som gäller för att en arbetsplats ska vara lämplig för distansarbete. Arbetsgivaren står för investerings- och driftskostnaderna för den nödvändiga utrustningen, operativsystemen, nyttoprogrammen samt datakommunikationsförbindelserna för distansarbetet.

Arbetsgivaren har rätt att fastställa kraven på den nödvändiga datatekniska utrustningen och programvarornas kompatibilitet så att systemen inte står i strid med arbetsplatsens datasystem.

Ett avtal ska alltid ingås mellan arbetsgivaren och arbetstagaren om distansarbete. Avtalet ska även gälla övervakning av arbetet, nödvändig kontroll av loggdata samt användarstöd.

8.4 Bekämpning av fientliga program och koder

Enheten ska förfoga över anvisningar om bekämpningen av fientliga program och koder. Separata instruktioner ska ges för servrar och enskilda arbetsstationer samt bärbara datorer. Enheten ska även utarbeta anvisningar för uppdateringen av virusdatabaser och hur de tas i bruk. Likaså ska det finnas anvisningar om hur störningssituationer ska anmälas.

8.5 Datateknisk kontroll

Den datatekniska kontrollen omfattar en driftsjournal. Enheten ska planera följande registreringsförfaranden om användningen av programvara (loggdata):

- uppföljning av felloggar och åtgärder
- att upptäcka intrång i systemet och åtgärder
- övervakning av systemet och nätet
- övervakning av användningen av en arbetsstation
- att upptäcka en felsituation och åtgärder.

8.6 *Återhämtningsplanering*

Återhämtningsplaneringen börjar med utarbetandet av en analys över avbrottseffekterna. Analysen fastställer kraven på servicenivå, målen för användbarheten samt tillåtna avbrottstider separat för varje system. Resultatet av analysen är en prioritetsklassificering av funktioner och system med vilken systemens resursbehov kan fastställas.

I återhämtningsplaneringen fastställs den operativa beredskapen och den tekniska beredskapen inklusive säkringen av datamaterialet. Återhämtningsplanen ska omfatta anvisningar om förfarandet när störningar och avbrott upptäcks, registreras och repareras. Ansvaret för alla uppgifter i planen ska fördelas antingen på den egna personalen inklusive reservpersoner eller på angivna personer hos serviceproducenten i det fall att enheten köper tjänsterna. Det ska också finnas anvisningar och ansvarsfördelning för ledningen i olika situationer.

8.7 *Datasäkerhet under undantagsförhållanden*

I planeringen av datasäkerheten under undantagsförhållanden ingår att fastställa uppgifterna inom enheten under undantagsförhållanden. Planeringen ska beakta hot mot verksamheten samt intressegruppernas behov av information eller informationsproduktion. På basis av enhetens prioritetsklassificering reserveras personal, lokaler, enheter, reservdelar och tillbehör för att upprätthålla beredskapen. Därtill utreds förfarandet för att trygga service och underhåll. Planeringen ska omfatta en beskrivning av förfarandet när man frångår användningen av datatekniken och återgår till att använda den i normala förhållanden.

9 Programvarusäkerhet

Programvarusäkerhet gäller upprätthållandet av operativsystemens, systemprogrammens samt tillämpnings- och datakommunikationsprogrammens säkerhet.

Hela programvarusäkerheten omfattar identifiering, isolering, passerkontroll och säkring av programvara, observation och avslöjanden, loggförfaranden samt kvalitetssäkring och säkerhetsåtgärder. När tjänster läggs ut ska en säkerhetsnivå som motsvarar den i den egna enheten eftersträvas.

9.1 Programsäkerhetsmål

Utöver att trygga åtkomsträttigheterna till programmen är syftet att trygga programvarans användbarhet i alla förhållanden. För att trygga programmens kvalitet och användbarhet ska man undvika gratisdistribuerade program. Enheten ska ha licens för alla program och de ska registreras enligt programproducentens anvisningar. Härigenom tryggas versions- och korrigeringsuppdateringar för programmen.

För att trygga datasäkerheten ska man utreda och se till att programmens skyddsegenskaper är tillräckliga för den miljö där programmen ska användas. Skyddsegenskaperna omfattar underhållsförfaranden, styrningen vid förändringar, ansvariga personer i enheten (ägare, systemadministratör, ansvarig för tekniskt underhåll) samt följande kontroller:

- inloggning
- övriga gränssnitt
- inmatning av data
- dataöverföring och -hantering
- lagring av data
- rapportering och utskrift.

I bilaga 4 presenteras en metod att fastställa systemets eller programvarans säkerhetsklass utgående från hur kritisk verksamheten är.

9.2 *Livscykelmodell*

En livscykelmodell illustrerar programmets eller programvarans livscykel från anskaffningsbeslutet ända tills programmet eller programvaran tas ur bruk och arkiveras med alla dokument och datasystemenheter. Även efter detta kan programmet eller programvaran behövas för sådana datahanteringsåtgärder som de nyare programmen inte kan hantera.

9.3 *Krypteringsprogram*

Med krypteringsprogram kan all överförbar datakommunikation, ett enskilt meddelande eller separat informationsmaterial krypteras. Policyn för användningen av krypteringsprogram beror på hur känsligt och kritiskt materialet är.

10 Informationsmaterialsäkerhet

Syftet med informationsmaterialsäkerheten är att säkerställa informationsmaterialets

- användbarhet
- integritet
- konfidentiella natur.

Informationsmaterialsäkerheten kan tryggas bl.a. genom en klassificering och förteckning av informationsmaterialet samt behörig styrning, hantering, lagring och förstöring av dataverktygen.

10.1 Informationsklassificering

Klassificeringen av informationsmaterial föreskrivs i lagen (621/1999, 18:4 §) och förordningen (1030/1999) om offentlighet i myndigheters verksamhet. I personuppgiftslagen (523/1999) bestäms separat om personuppgifter och hanteringen av uppgifterna.

I lagen om integritetsskydd i arbetslivet (759/2004) föreskrivs om behandlingen av arbetstagares personuppgifter, test och kontroller som gäller arbetstagare samt om de krav som ställs på dessa, teknisk övervakning på arbetsplatsen samt om hämtning och öppnande av arbetstagares elektroniska meddelanden. Lagen omfattar förfaranden och sekretesspraxis vid behandling av arbetsgivarens uppgifter och uppgifter som hör till arbetstagaren.

10.2 Skydd, säkring och återhämtning av informationsmaterial

Med skydd av informationsmaterial avses skydd av material i pappersform och därtill skydd av elektronisk eller muntlig information. Kravnivån för skyddsmetoderna beror på klassificeringen av informationsmaterialet. Utöver den fysiska hanteringsmiljön för konfidentiell information ska man beakta hur arbetsstationen används antingen i enhetens egna lokaler eller med en bärbar arbetsstation utanför enheten. Kravet är att skydda behandlingen av konfidentiell information så att obehöriga inte har åtkomst till uppgifterna. Detta gäller även muntlig information antingen i eller utanför enhetens lokaler.

Med hjälp av lösenord samt policy och förfaranden med åtkomsträttigheter fastställs och skyddas åtkomsträttigheterna till enhetens olika operativsystem, till lokaler där informationen hanteras samt till själva informationen. För användaren är den s.k. ”single sign on” metoden det enklaste. Det betyder att användaren med en användarkod och ett lösenord kan logga in till filer och system som ingår i användarens åtkomsträttigheter.

Den enklaste formen av informationssäkring är att spara informationen med jämna mellanrum under arbetets gång på arbetsstationens hårdskiva, på en server eller annan lagringsutrustning. Härigenom försäkrar man sig om att informationen förvaras och kan användas om materialet av någon anledning förstörs mitt under hanteringen.

Enhetens livsviktiga och konfidentiella säkerhetsklassificerade information och/eller säkerhetskopia av informationen ska förvaras på ett brand- och inbrottssäkert ställe, till exempel i ett brandskyddsklassificerat kassaskåp. När det gäller säkerhetskopior på lagringsutrustning ska anvisningarna om hanteringen och förvaringen av elektroniska arkiv iakttas. Informationens integritet förutsätter att elektroniskt lagrat material kopieras regelbundet med bestämda årsintervaller på ny lagringsutrustning.

Med dagens metoder kan man oftast nästan helt återställa t.ex. information på en brandskadad arbetsstations hårddisk.

10.3 Datamaterialets arkiveringsskydd

När information och informationsmaterial arkiveras ska man beakta de lagstadgade kraven på förvaringstider och –sätt (arkivlagen 831/1994). Utöver bestämmelserna och anvisningarna om arkiveringen av social- och hälsovårdens uppgifter ska enheten ha anvisningar om förvaringen och arkiveringen av övriga konfidentiella uppgifter och dokument. Lagen förutsätter att enheten har en person som är ansvarig för arkivfunktionen.

Enligt lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) ska klientuppgifterna behandlas så att uppgifternas åtkomst och användbarhet tryggas. Klientuppgifterna ska förvaras oskadade och oförändrade under hela förvaringstiden. Tjänsteproducenten ska samla in loggуppgifter om all användning av klientuppgifterna och om varje överlåtelse av klientuppgifterna.

Den som producerar tjänster för den offentliga hälso- och sjukvården ska enligt lagen registrera sig som användare av de riksomfattande datasystemtjänsterna. På samma sätt ska även den som producerar tjänster för den privata hälso- och sjukvården registrera sig ifall patienthandlingarna långtidsförvaras elektroniskt.

Informationsteknikens metodutveckling ska beaktas när det gäller arkivering och återhämtning av uppgifter. Enheten ska säkerställa användbarheten och integriteten även av gamla uppgifter som är viktiga för enheten genom att spara de operativ- och datasystem som användes då uppgifterna producerades samt eventuellt den tidens dator eller databehandlingsenhet så att uppgifterna kan återhämtas och bearbetas så att de blir kompatibla med de nya operativ- och datasystemen.

10.4 Förstöring av datamaterial

Enhetens informationsskyddsinstruktioner ska innehålla en beskrivning av hur information förstörs. Instruktionerna utgör samtidigt en del av verksamhetsenhetens avfallsinstruktioner. Informationen förstörs enligt dess konfidentiella nivå. Förstöringens hela logistikkedja ska beskrivas i enhetens anvisningar. Ifall datasekretessbelagt avfall sänds till en utomstående serviceproducent för förstöring ska man föra bok över varje post som förstörs, och metoden ska då och då utvärderas externt för att man ska kunna försäkra sig om att systemet är vattentätt.

I bilaga 5 presenteras en tabell i finansministeriets anvisning VAHTI över metoder att förstöra olika typer av informationsmaterial.

11 Maskinvarusäkerhet

Syftet med maskinvarusäkerhet är att se till att maskinvaran och informationsegendomen inte skadas och att förhindra att de försvinner.

Maskinvarusäkerheten omfattar användbarhet, funktion, montering, underhåll, återvinning, makulering och kvalitetssäkring av maskinvara för databehandling och datakommunikation.

11.1 Maskinvara, tillbehör och anskaffningar

Innan anskaffningarna planeras och genomförs ska man se till att maskinvaran är kompatibel och lämplig och enligt detta fastställa de krav som maskinvaran ska uppfylla. I systembeskrivningen ingår servrar och centralenheter, intranätets routrar, arbetsstationer, bärbara datorer, trådlösa nät samt övrig maskinvara.

I livscykelinspektionen ska maskinvarans livslängd fastställas på förhand. Därtill ska man se till att maskinvaran kan förnyas eller expanderas och att det finns stöd för underhåll och service.

Apparaterna ska registreras och stöldmärkas. Ansvariga personer ska utses för apparaterna.

Maskinvarans egna program ska få versions- och korrigeringsuppdateringar.

I maskinvarusäkerheten ingår även planer för återvinning och förstöring.

När information arkiveras elektroniskt ska enheten se till att uppgifterna även senare är tillgängliga vid behov. Därför ska man spara gamla datasystemapparater med tillhörande programvara.

11.2 Bärbara datorer

Enheten ska ge anvisningar om användningen och förvaringen av bärbara datorer. Vid anskaffningen av en bärbar dator är det skäl att välja en modell som kan förses med en låsbar stöldvajer. Anvisningar ska också ges om användningen av stöldvajer även i användarens egna utrymmen.

När en bärbar dator används för distansarbete antingen med en fast eller en trådlös förbindelse ska förbindelsen skyddas med ett VPN-system. Utgångspunkten är att ingen sekretessbelagd eller konfidentiell information lagras på

den bärbara datorns hårdskiva. Arbetet på en bärbar dator sker med hjälp av distansförbindelsen och all information som bearbetas ska finnas tillgänglig på enhetens server och sparas på servern. Motsvarande säkerhetsförskrifter ska tillämpas på bearbetningen av lagrad sekretessbelagd information på CD-ROM-skivor eller annan elektronisk datalagringsutrustning (till exempel en extern hårdskiva).

11.3 Datateknikservice

Datateknikservicen ska ske så att servicepersonal som kommer till kontorslokalerna eller som befinner sig på annat håll utanför kontorslokalerna inte kan få tillgång till sekretessbelagd information. En datasäkerhetsförpliktelse kan begäras av servicepersonalen. Den förpliktar personalen att följa lagenligt förfarande, låta bli att utnyttja information som av misstag kommit till personalens kännedom eller avslöja att en person har åtkomst till denna information.

12 Kränkning av datasäkerheten

Vid en kränkning av datasäkerheten har enhetens egen information eller information som enheten administrerar råkat i händerna på obehöriga personer eller någon har avsiktligt eller oavsiktligt genom sitt förfarande förhindrat att enhetens uppgifter behandlas på det sätt som enheten föreskriver och på enhetens egen datautrustning eller på en datautrustning som enheten administrerar.

12.1 Sanktioner vid kränkning av dataskyddet

Obehörig användning av information, intrång i datasystem eller störning av databehandling kränker databehandlingens integritet. Det är viktigt att förhålla sig allvarligt till upptäckta fall eftersom strafflagen skyddar en kränkt rätt. I lindriga fall kan ärendet lösas genom interna disciplinära åtgärder. Grava fall, som t.ex. obehörig överlåtelse av personuppgifter, kan leda till myndighetsåtgärder. I alla fall ska förseelserna anmälas till enhetens ledning och personer som ansvarar för datasäkerheten.

Brott mot datasäkerheten kan indelas enligt effekt på följande sätt:

- brott mot databehandlingsfrid, förhindrande av databehandling
- obehörig användning av information
- obehörig användning av datasystem, operativsystem eller program.

Brott mot dataskyddet är ett målsägandebrott, och för att ärendet ska anhängiggöras förutsätter det i regel att den person vars uppgifter använts obehörigt gör en brottsanmälan. Polisen kan tillfälligt tillvarata handlingar, arbetsstationer, servrar eller lagringsutrustning som anses nödvändiga för polisundersökningen.

12.2 Observations-, rapporterings- och hanteringsförfarandet vid kränkning av dataskyddet

Vid en kränkning av dataskyddet utreds skadan och effekterna av kränkningen. Detta kan i allmänhet undersökas direkt på datorn eller servern på följande sätt:

- Användningen av datorn eller servern förhindras genom att rättigheterna till användarkoden eller den skadliga IP-adressen (IP = datorns kod) spärras under utredningen.
- Användningen av koden kontrolleras och användningen sparas i loggen som bevismaterial och man ser till att användningen av koden inte riskerar det övriga systemets datasäkerhet eller användbarhet.

En kränkning av dataskyddet och ett brott mot dataskyddet ska alltid utredas internt, dock så att sekretessbelagd information inte avslöjas mer än nödvändigt under utredningsarbetet.

Betydelsen av sanktionerna vid brott mot dataskyddet eller datasäkerheten är begriplig och verkställandet klart och tydligt om enheten har en färdigt planerad datasäkerhetspolicy, konsekvent definierade personliga ansvar och entydiga procedurregler samt en utbildad personal.

DATASÄKERHETEN I LAGSTIFTNINGEN

1. Allmänna bestämmelser om datasäkerheten

1.1 Bestämmelser om informationsmaterial

Grundlagen (731/1999)

- skydd för privatlivet (10 §)
- yttrandefrihet och offentlighet (12 §)

Personuppgiftslagen (523/1999)

- skydd för privatlivet samt övriga grundläggande fri- och rättigheter som tryggar skyddet
  för den personliga integriteten (1 §)
- datasäkerhet och förvaring av uppgifter (32-35 §)

Lag om offentlighet i myndigheternas verksamhet (621/1999)

- offentlighetsprincipen (1 §)
- skyldighet till en god informationshantering (3 §)
- rätt att ta del av en sekretessbelagd handling (10 §)
- en parts rätt att ta del av en handling (11 §)
- myndigheternas skyldighet att främja möjligheterna att ta del av en handling samt en god informationshantering (17 §)
- god informationshantering (18/1999)
- skyldighet att iaktta sekretess (22 § - 25 §)
- handlingssekretess (22 §)
- tystnadsplikt och förbud mot utnyttjande (23 §)
- sekretessbelagda myndighetshandlingar (24 §)
- undantag från och upphörande av sekretess (26 §-32 §)

Förordning om offentlighet och god informationshantering i myndigheternas verksamhet (1030/1999)

- utredningar i syfte att genomföra god informationshantering (1 §)
- klassificering av särskilt känsligt datamaterial (2 §)
- allmänna datasäkerhetsåtgärder i fråga om särskilt känsligt material (3 §)
- anvisningar, övervakning och uppföljning (4 §)
- beskrivning av datasystem (8 §)

Arkivlag (831/1994)

- tillgänglighet och förvaring, förstöring av onödigt material (7 §)
- skydd mot förstörelse, skada och obehörig användning (12 §)

Lag om säkerhetsutredningar (177/2002)

- lagens tillämpningsområde (1 §)
- normal säkerhetsutredning, sökande (4 §)
- genomförande av en säkerhetsutredning; bygger på registeruppgifter (8 §)
- säkerhetsklassificering (14 §)
- genomförande av en omfattande säkerhetsutredning (15 §)
- syftet med en begränsad säkerhetsutredning (19 §)

Inrikesministeriets förordning om ansökningsförfarandet vid säkerhetsutredningar (710/2002)

Lag om kontroll av brottslig bakgrund hos personer som arbetar med barn (504/2002)

- arbetsgivarens skyldighet att kräva uppvisande av straffregisterutdrag (3 §)
- straffregisterutdrag beträffande dem som producerar privat socialservice eller privata hälso- och sjukvårdstjänster (4 §)
- anteckning om uppvisat straffregisterutdrag och återlämnande av utdraget (7 §)
- tystnadsplikt (8 §)

Förvaltningslag (434/2003)

- tystnadsplikt för ombud och biträden (13 §)
- hur en handling sänds till en myndighet och hur ett förvaltningsärende inleds (16 § – 22 §)

1.2 Bestämmelser om informationsmaterial och informationsteknik

Lag om elektronisk kommunikation i förvaltningsärenden (1318/1999)

- certifieringsverksamhet (4 § - 12 §)
- anordnande av elektronisk service, datasäkerhet (18 §)
- anhängiggörande med en elektronisk handling (22 §)

Lag om utnyttjande av elektronisk telekommunikation och automatisk databehandling vid domstolar (594/1993)

Lag om elektroniska signaturer (14/2003)

- användningen av elektroniska signaturer och tillhandahållandet av produkter för elektroniska signaturer och tjänster i anslutning till dem samt datasekretessen och dataskyddet vid elektronisk handel och elektronisk kommunikation.

Lag om elektronisk kommunikation i myndigheternas verksamhet (13/2003)

- anhängiggörande, behandling och delgivning av förvaltningsärenden, domstolsärenden, åtalsärenden och utsökningsärenden på elektronisk väg
- främjande av elektroniska dataöverföringsmetoder för att göra uträttandet och behandlingen av ärenden smidigare och snabbare

Lag om integritetsskydd i arbetslivet (759/2004)

- behandling av arbetstagares personuppgifter, test och kontroller som gäller arbetstagare, teknisk övervakning på arbetsplatsen samt om hämtning och öppnande av arbetstagares elektroniska meddelanden

Lag om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (565/1999)

- dataskydd inom televerksamhet(4 §)
- Teleföretagets datasäkerhetsskyldigheter (6 §)
- teleoperatörernas tystnadsplikt (7 §)
- begränsningarna för direktmarknadsföring (21 §)

Förordning om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (723/1999)

Lag om ändring av lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet(459/2002)

- identifiering av direktmarknadsföring (21 a §)

Telemarknadslag (396/1997) och lag om ändring av telemarknadslagen (566/1999)

- förbud mot avkodningssystem (25 §)

Lag om registerförvaltningen (166/1996)

Strafflagen inklusive ändringar (578/1995, 951/1999)

- olovlig användning (28 kap. 7 § - 9 §)
- skadegörelse (35 kap. 1 § - 3 §)
- kränkning av kommunikationshemlighet (38 kap. 3 §)
- dataintrång (38 kap. 8 §)

- brott mot tjänstehemlighet (40 kap. 5 a §)
- förorsakande av fara för databehandling (34 kap. 9 a §)

Tvångsmedelslag (450/1987) inkl. ändringar (18/2003, 64/2003, 646/2003)

- förutsättningar för teleavlyssning (2 §)
- förutsättningar för teleövervakning (3 §)
- förutsättningar för teknisk observation (4 §)
- bestämning och registrering av DNA-profiler (5 §)
- förutsättningar för teleavlyssning (2 §)
- 1 kap. Gripande, anhållande och häktning; förutsättningar för anhållande (3 §)
- 5 kap. Husrannsakan; Husrannsakan för att söka efter föremål (1 §)
- 5 a kap. Teleavlyssning, teleövervakning och teknisk observation; (1 § – 3 §, 3a §, 4 §, 4 a §, 4 b §, 5 §)

Polislag (493/1995)

- 3 kap. Stadganden om inhämtande av information (28 § - 36 §)
- tystnadsplikt (43 §)
- rätt att förtiga uppgifter (44 §)

Upphovsrättslag (404/1961)

- upphovsrätt till programvara (Lag om ändring av upphovsrättslagen 446/1995)
- användningen av databaser (Lag om ändring av upphovsrättslagen 250/1998)

Lag om tillhandahållande av informationssamhällets tjänster (458/2002)

- uppfyllande av formkraven för avtal på elektronisk väg (12 §)
- ansvarsfrihet vid överföring av information och vid tillhandahållande av tillgång till kommunikationsnät (13 §)
- ansvarsfrihet vid lagring av information i cacheminne (14 §)
- ansvarsfrihet vid lagring av information (15 §)
- förordnande om spärrning av information (16 §)
- innehållsproducentens rättsskydd (18 §)

2. Bestämmelser om beredskapen i undantagsförhållanden

Beredskapslag (1080/1991)

Lag om tryggande av försörjningsberedskapen (1390/1992)

Statsrådets beslut om målen med försörjningsberedskapen (350/2002)

- Målen med beredskapen, samhällets tekniska infrastrukturer

3. *Särskilda bestämmelser om social- och hälsovårdens funktioner*

Lag om patientens ställning och rättigheter (785/1992) inklusive ändringar (489/1999, 653/2000, 411/2001)

- patientens rätt till information (5 §)
- rätt till information samt behörighet (9 §)
- journalhandlingar och annat material som hänför sig till vård och behandling (12 §)
- sekretessbelagda uppgifter i journalhandlingarna (13 §)
- brott mot tystnadsplikt (14 §)

Lag om klientens ställning och rättigheter inom socialvården (812/2000)

- klientens rätt att få en utredning om åtgärdsalternativen (5 §)
- utlämnande av uppgifter till klienten eller dennes företrädare (11 §)
- klientens och företrädarens skyldighet att lämna uppgifter (12 §)
- handlingssekretess (14 §)
- tystnadsplikt och förbud mot utnyttjande (15 §)
- samtycke till utlämnande av uppgifter (16 §)
- utlämnande av sekretessbelagda uppgifter för tryggande av vården av och omsorgen om klienten (17 §)
- utlämnande av sekretessbelagda uppgifter i vissa andra situationer oberoende av klientens samtycke (18 §)
- undantag i fråga om och upphörande av sekretess (19 §)
- Skyldighet att lämna sekretessbelagda uppgifter till socialvårdsmyndigheten (20 §)
- utlämnande av uppgifter med hjälp av teknisk anslutning (21 §)
- socialvårdsmyndighetens rätt att få handräckning (22 §)
- behandling och förvaring av handlingar (26 §)
- tillämpningsområdet för bestämmelserna om datasekretess och handräckning (27 §)
- anteckning om inhämtande eller utlämnande av uppgifter (28 §)
- straffansvar (29 §)

Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007)

- klientuppgifternas användbarhet och förvaring (4 §)
- uppföljning av användning och utlämnande (5 §)
- Journalhandlingarnas datastrukturer (6 §)
- identifiering (8 §)
- elektronisk signering av handlingar (9 §)

- Utlämnande av patientuppgifter (10 §)
- sökuppgifter (11 §)
- förbud mot utlämnande av sökuppgifter (12 §)
- patientens samtycke (13 §)
- Riksomfattande informationssystemtjänster (14 §)
- skyldighet att ansluta sig som användare av informationssystemtjänsterna (15 §)
- ansvar vid skötseln av informationssystemtjänsterna (16 §)
- information till patienten (17 §)
- klientens rätt att få uppgifter (18 §)
- åtkomst till uppgifter (19 §)
- styrning, övervakning och uppföljning (20 §)
- straffbestämmelser (23 §)

Social- och hälsovårdsministeriets förordning om upprättande av journalhandlingar samt om förvaring av dem och annat material som hänför sig till vård (99/2001)

- förordningens tillämpningsområde (1 §)
- journalhandlingar (2 §)
- den registeransvariges allmänna förpliktelser (3 §)
- rätt att använda uppgifter i journalhandlingar (4 §)
- anskaffning av service från någon annan (5 §)
- rätt att göra anteckningar i journalhandlingar (6 §)
- centrala principer och krav beträffande anteckningar i journalhandlingar (7 §)
- basuppgifter som antecknas i journalhandlingarna (10 § - 21 §)
- förvaring av journalhandlingar (22 § - 23 §)

Lag om elektroniska recept (61/2007)

- lagens syfte (1 §)
- lagens tillämpningsområde (2 §)
- definitioner (3 §)
- information till patienten (4 §)
- informationen i recept (6 §)
- signering av recept (7 §)
- kryptering av recept (8 §)
- patientanvisning (9 §)
- apotekets rätt att få uppgifter (11 §)
- expediering av elektroniska recept (12 §)
- läkares och tandläkares rätt att få uppgifter (13 §)
- utlämnande av uppgifter till myndigheter (15 §)
- patientens rätt till information (16 §)
- åtkomst till uppgifter (17 §)

- förvaring av uppgifterna (19 §)
- den datatekniska hanteringen av elektroniska recept (20 §)
- recept- och expedieringsprogramvara (21 §)
- införande av elektroniska recept (23 §)
- styrning, uppföljning och övervakning (24 §)
- avgifter (25 §)
- straff- och hänvisningsbestämmelser (26 §)

Förordningen om yrkesutbildade personer inom hälso- och sjukvården (546/1994)

(Verksamhetsenhet)

DATASKYDDSANVISNINGAR (modell)

(Ges till en person som ingått en förbindelse)

Nyttjanderätten till arbetsstationer (inklusive ADB-utrustning ansluten med en fast/trådlös förbindelse till datanätet), telekommunikationsnätet och adb-systemen ges endast till personer som undertecknat denna sekretess- och användarförbindelse.

1. Sekretess

- Under eller efter utgången av en anställning/annat arbetsuppdrag får arbetstagaren inte ge en utomstående eller obehörig person konfidentiell eller sekretessbelagd information angående (verksamhetsenheten), dess underavdelningar, kunder, avtalspartner eller andra samarbetsinstanser som den anställda fått i arbetet. Utöver patient-/klientuppgifter (om hälsotillstånd) gäller detta även affärs- och yrkeshemligheter samt uppgifter om säkerhets- och beredskapsarrangemang.
- Läs- eller åtkomsträttigheten till register gäller inte andra uppgifter än de som arbetsuppdraget kräver.
- Sekretessplikten (dokumentsekretess och tystnadsplikt) bestäms i flera lagar.
- Lag om patientens ställning och rättigheter (785/1992, ändrad 653/2000, 13 §) och Lag om klientens ställning och rättigheter inom socialvården (812/2000)
- Lag om offentlighet i myndigheternas verksamhet (621/1999, 24 §)
- Personuppgiftslagen (523/1999, 33 §)
- Enligt patientuppgiftslagen/lagen om klientens ställning och rättigheter inom socialvården är patientuppgifterna/klientuppgifterna sekretessbelagda

2. Användarkod och lösenord

- Användarkoderna är personliga. Ett undantag utgörs av en gruppanvändarkod i begränsad användning på en enda arbetsstation. Koden innehas alltid av en ansvarig person i vars namn koden beviljats. Var och en ansvarar med sin användarkod för införda anteckningar och händelser. När anställningen upphör fråntas åtkomsträttigheterna automatiskt.
- Ett lösenord ska bytas omedelbart när det beviljats och senare med överenskomna intervaller eller vid behov.

- Användarkoden och lösenordet ska hemlighållas. De får inte ges till någon annan. Arbetsgivaren frågar aldrig efter användarkoden eller lösenordet.

3. Användningen av en arbetsstation

- Arbetsstationen är avsedd att användas endast för arbetsuppdrag.
- I ringa utsträckning är det tillåtet att använda den för personliga ändamål med chefens tillstånd.
- Endast program som godkänts av enheten och med enhetens licens, program som installerats och stöds av resultatområdets informationsförvaltning eller som installerats och stöds enligt godkännande av den ansvariga enheten inom resultatområdets informationsförvaltning får användas på arbetsstationen.
- Inställningar som den ansvariga enheten inom resultatområdets informationsförvaltning infört får inte ändras. Detta gäller även skärmsläckare och bakgrundsbilder.
- De program som verksamhetsenheten skaffat får inte kopieras.
- Arbetsstationen får inte anslutas till nätet eller flyttas till en annan arbetsplats utan tillstånd. Detta gäller även bärbara datorer.
- Omedelbart efter avslutat arbete ska man logga ut ur datasystemen eller låsa arbetsstationen även när man avlägsnar sig från arbetsstationens omedelbara närhet och inte kan övervaka arbetsstationen.
- Arbetsstationen får användas endast med egen användarkod och eget lösenord.
- Det är inte tillåtet att använda samma disketter eller annan datorutrustning på arbetsplatsen och utanför arbetsplatsen ifall man inte kontrollerat att de säkert är virusfria.
- När man använder arbetsstationen ska man beakta datanätets och servrarnas begränsade kapacitet. Bilder, grafik och ljudfiler får sändas i nätet eller sparas på servern endast om arbetsuppgifterna kräver det.
- Vid misstanke om att arbetsstationen blivit smittad av ett datavirus ska man omedelbart avsluta arbetet på arbetsstationen.
- Arbetsstationen får inte användas för bestående lagring av filer.
- Varje användare ansvarar själv för säkerhetskopieringen av filer som lagrats på arbetsstationen. (Säkerhetskopieringen av filer på servern utförs centrerat eller av systemadministratören).

4. Användningen av e-post och internetförbindelser

- När en internet/www-browser används samlas det logg- och säkerhetsinformation som kontrolleras regelbundet.
- Det är inte tillåtet att kopiera program från internet.
- Känsliga och andra konfidentiella uppgifter får inte sändas via en extern e-post.

- På grund av virusrisken får bifogade filer som sänts via en extern e-post inte öppnas om meddelandet kommer från en obestämd källa. Meddelandet ska raderas.
- E-post (t.ex. förnamn.efternamn@hus.fi) får inte automatiskt styras utanför verksamhetsenheten.
- E-postkedjebrev och annan s.k. skräppost får inte sändas eller vidareförmedlas, de ska förstöras.

5. Systemanvisningar

- Varje användare ska studera verksamhetsenheten och den egna enhetens dataskyddsanvisningar och bruksanvisningarna för de datasystem som han/hon använder samt registrens registerbeskrivningar.
- Användningen av datasystemen lämnar fingermärken efter sig, och användningen kontrolleras.

6. Påföljder

- Vid brott mot reglerna och principerna i förbindelsen återtas åtkomsträtten till datasystemen för en bestämd tid eller tillsvidare, tills förseelsen behandlats.
- Förseelser anmäls alltid till chefen. Om det gäller en avsiktlig eller allvarlig förseelse ska fallet vidarebehandlas. Ifall den avsiktliga förseelsen direkt eller indirekt leder till ekonomiska förluster är förövaren även skadeståndsskyldig.
- Missbruk av information eller avsiktliga regelbrott kan därtill leda till straffrättsliga påföljder.

7. Anmälningsskyldighet

- Datavirus ska alltid anmälas till den ansvariga enheten för resultatområdets dataförvaltning.
- Alla obestämda förfrågningar om användarkod och lösenord ska omedelbart anmälas till den ansvariga enheten för resultatområdets dataförvaltning (adb-stöd).
- Alla observerade brott eller försök till brott mot dataskyddet ska omedelbart anmälas till den ansvariga enheten för resultatområdets dataförvaltning (adb-stöd).

8. Arbetsgivarens skyldighet

- (Enhetens namn)s skyldighet som arbetsgivare är att skydda sina anställda mot kränkningar av datasäkerheten och dataskyddet.

Förbindelsen ingicks / 200……..

(Verksamhetsenhet)_____

SEKRETESS- OCH ANVÄNDARFÖRBINDELSE (modell)

Jag har studerat den nu gällande sekretess- och användarförbindelsen för _____ datasäkerhetspolicyn och nvisningarna samt dataskyddsplikterna för _____

Jag förbinder mig att följa dem liksom även övriga separat angivna anvisningar och bestämmelser om sekretess och datasäkerhet.

Jag har läst och förstått principerna i sekretess- och användarförbindelsen och förbinder mig att följa dem.

Arbetsplats

Datum / 200

Underskrift _____

Namnförtydligande _____

Personbeteckning _____

Difgfot!voefstlsjgu _____

☐ Datasäkerhetsanvisningarna utfärdade

Denna förbindelse förvaras under anställningstiden och arkiveras tio år efter avslutad anställning.

BESTÄMNING AV SYSTEMSÄKERHETSKLASS UTGÅENDE FRÅN HUR KRITISK VERKSAMHETEN ÄR

Säkerhetsklassen (kritiskheten) hos ett datasystem/en informationshanteringsmetod under arbete utreds på basis av effekterna på verksamheten:

- beskrivning av ett system under arbete/ en databehandlingsmetod som ska tas i bruk
- utredning av system och mekanismer som påverkar valet av säkerhetsnivå
- utredning av system eller metoder som påverkas av valet av det aktuella systemets säkerhetsnivå
- utgångspunkterna för en utvärdering av systemet under arbete bestäms:
  - systemets krav på användbarhet och problemens inverkan på verksamheten
    - maximilängden på driftsavbrott högst (aldrig, max. minuter, max. timmar, max några dagar, max en vecka, flera veckor)
  - systemets krav på integritet och problemens inverkan på verksamheten
  - inverkan av störningar i konfidentialiteten på verksamheten
- eventuella preciserande frågor och synpunkter som inverkar på bestämningen av systemets/databehandlingsmetodens säkerhetsklass.

FÖRSTÖRING AV SEKRETESSBELAGD INFORMATION OCH HANDLINGAR

Data-material	Säkerhetsklass			
	Offentligt	Icke-offentlig/ sekretessbelagd		
		Konfidentiellt	Hemligt	Synnerligen hemligt
Pappers-material	Sänds för återvinning	Skärs i max. 4x60 mm stora strimlor med en korsskärande dokumentförstörare före återvinning (DIN standard 32757, säkerhetsklass 3)		Skärs i max. 0,8 x 15 mm strimlor (DIN standard 32757, säkerhetsklass 5)
Mikro-filmer	Innehåller silver:	Förstörs i specialaffärer för silvereliminering eller bränns i problemavfallsanläggningar		Skärs i strimlor på max. 0,2 x 0,2 mm (DIN standard 32757, säkerhetsklass 5, mikrofilmer)
	Innehåller inte silver:	Skärs i strimlor på max. 1 x 1 mm (DIN standard 32757, säkerhetsklass 3, mikrofilmer)		Förstörs som andra mikrofilmer
		Mikrofilmavfallet sänds till avfallsplatsen enligt avfallslagen		
Magnetisk datautrustning	Förstörs genom formatering	Se till att formateringen faktiskt förstör informationen och inte bara frigör plats.		Förstöring genom att skivorna och disketterna bryts sönder, magnetband och kassettband strimlas
	Dataskydds-klassificerad information:	Förstörs genom att man skriver tecken på den frigjorda platsen med för ändamålet lämpliga program		
	Kassetter, magnetband och disketter:	Genom demagnetisering OBS! Sekretessbelagd information ska krypteras på en databärare. Förstöring genom att skivorna och disketterna bryts sönder, magnetband och kassettband strimlas. Avfallet sänds till avfallsplatsen enligt avfallslagen		
Övriga databärare	Ytterligare information:	Dataombudsmannens kansli och Arkivväsendet		

INFORMATIONSKÄLLOR

Publikationer utgivna av Ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI):

1. Rekommendation om. datasäkerheten i samband med statligt distansarbete, VAHTI 1/1999
2. Datasäkerhetsrekommendation för externalisering av dataförvaltningsfunktioner, VAHTI 2/1999
3. Datasäkerhetsbegrepp inom statsförvaltningen, VAHTI 1/2000
4. Datasäkerhetsanvisning om hantering av statens datamaterial, VAHTI 2/2000
5. Datasäkerhetsrekommendation för utveckling av datasystem, VAHTI 3/2000
6. Allmän anvisning för skydd mot datorvirus och andra skadliga program, VAHTI 4/2000
7. Allmän anvisning om datasäkerhetsarbetet vid statliga myndigheter, VAHTI 1/2001
8. Datasäkerhetsrekommendation för statsförvaltningens lokalnät, VAHTI 2/2001
9. Statsförvaltningens datasäkerhetsrekommendation för krypterings--praxis, VAHTI 3/2001
10. Allmän anvisning om datasäkerheten i samband med elektroniska tjänster och elektronisk kommunikation, VAHTI 4/2001
11. Hantering av e-post och logguppgifter, VAHTI 5/2001
12. Kontrollista för datateknikupphandlingarnas datasäkerhet, VAHTI 6/2001
13. Åtgärder vid kränkning av datasäkerheten, VAHTI 7/2001
14. Säkerhetsrekommendation för datatekniska anläggningslokaler, VAHTI 1/2002
15. Datasäkerhetsanvisning för statens distansarbete, VAHTI 3/2002
16. Principerna för hantering av konfidentiella internationella datamaterial, VAHTI 4/2002
17. Internet-datasäkerhetsanvisning för statens dataförvaltning, VAHTI 1/2003
18. Rekommendation om säker distansbrukararkitektur, VAHTI 2/2003
19. Bedömning av hanteringssystem för datasäkerheten, VAHTI 3/2003
20. Datasäkerhetsbegrepp inom statsförvaltningen, VAHTI 4/2003
21. Datasäkerhetsanvisning för användaren, VAHTI 5/2003
22. Guide för ordnandet av datasäkerhetsutbildning inom statsförvaltningen, VAHTI 6/2003

23. Anvisning om riskbedömning för främjandet av datasäkerheten inom statsförvaltningen, VAHTI 7/2003
24. Utvecklingsprogram för statsförvaltningens datasäkerhet 2004-2006, VAHTI 1/2004
25. Datasäkerhet och resultatstyrning, VAHTI 2/2004
26. Allmän anvisning om skydd mot fientliga program, VAHTI 3/2004
27. Tryggandet av statsförvaltningens främsta datasystem, VAHTI 4/2004
28. Statsförvaltningens e-postanvisning, VAHTI 1/2005
29. Information om statens dataadministration och datateknik 2004, VAHTI 2/2005
30. VAHTIs verksamhetsberättelse 2005, VAHTI 1/2006
31. Electronic Mail-handling Instruction for State Government, VAHTI 2/2006
32. Rapport om fördelningen av statsförvaltningens dataskyddsresurser, VAHTI 3/2006
33. Rapport om statsförvaltningens dataskyddsverksamhet dygnet runt, VAHTI 4/2006
34. Anvisning om datasäkerheten inom ärendehanteringen, VAHTI 5/2006
35. Uppställning och mätning av målen för dataskyddet, VAHTI 6/2006
36. Förändring och datasäkerhet – från regionalisering till externalisering – en kontrollerad process, VAHTI 7/2006
37. Bedömning av datasäkerheten inom statsförvaltningen, VAHTI 8/2006
38. Principerna och god praxis för förvaltningen av användarrätter, VAHTI 9/2006
39. Personalens datasäkerhetsanvisning, VAHTI 10/2006
40. Handbok för dataskyddsutbildare, VAHTI 11/2006
41. Identifiering i den offentliga förvaltningens nättjänster, VAHTI 12/2006
42. Datasäkerhetens resultatstyrning och utvecklingsredskap, VAHTI 1/2007

www.vn.fi

ISO/IEC 17799:fi; Informationsteknologi. Säkerhet. Anvisning för hantering av datasäkerheten. Finlands Standardiseringsförbund SFS.

ISO/IEC 27001:FI; Informationsteknologi. Säkerhet. Hanteringssystem för datasäkerheten. Krav. Finlands Standardiseringsförbund SFS.

Principerna och god praxis för hanteringen av datasäkerheten och dataskyddet i social- och hälsovårdens datasystem. Anvisning för social- och hälsovårdens

organisationer och verksamhetsenheter om utvecklandet av datasystemens datasäkerhet och dataskydd; STAKES, Rapporter 5/2005, Tero Tammisalo, Helsingfors 2005.

Handbok för social- och hälsovården om administreringen av organisationens datasäkerhet. Anvisning för social- och hälsovårdens organisationer och verksamhetsenheter om administreringen av datasäkerheten och utvecklandet av administreringsmetoderna. STAKES, Tero Tammisalo, duplikat.

SOCIAL- OCH HÄLSOVÅRDSMINISTERIETS PUBLIKATIONER
ISSN 1236-2050

2008: 1 Urpo Kiiskinen, Tuulikki Vehko, Kristiina Matikainen, Sanna Natunen, Arpo Aromaa. Terveyden edistämisen mahdollisuudet - vaikuttavuus ja kustannusvaikuttavuus.
ISBN 978-952-00-2503-8 (nid.)
ISBN 978-952-00-2504-5 (PDF)

2 Utarbetande av en datasäkerhetsplan. Handbok för verksamhetsenheter inom social- och hälsovården. (Vain verkossa).
ISBN 978-952-00-2507-6 (PDF)